Using Software Full Disk Encryption and Disk Partitioning to Protect and Isolate Network Attached Storage Functions

Read About

Network attached storage

NAS protocols

Block data – iSCSI

Packet Capture (PCAP)

Net-booting

Disk partitioning

Full disk encryption

LUKS

AES-256

Introduction

Unmanned vehicles are ideal for intelligence, surveillance, and reconnaissance (ISR) missions due to the amount of data a vehicle can gather without the risk to human life. As they are increasingly being used to gather large amounts of different types of data, the need for data storage versatility and data security rises. However, the risk of data loss or corruption grows as the number of systems using different protocols connecting to the device rises. Additionally, as the use of unmanned vehicles for deployed applications increases, so does the risk of highly sensitive data being lost or captured in hostile territory. Through disk partitioning and commercial off-the-shelf (COTS) data-at-rest (DAR) encryption, this paper proposes a solution that reduces risk of data loss, corruption, and accessibility if intercepted.

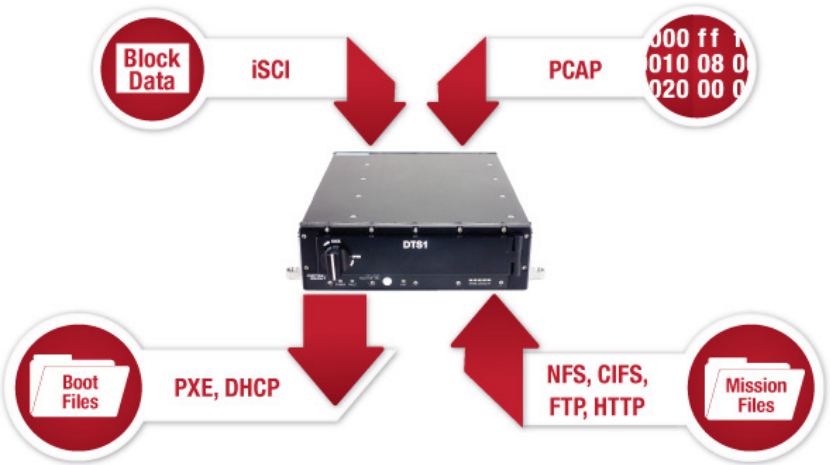

Figure 1: DTS1 Network attached storage protocol support

Most modern unmanned vehicles, ISR aircraft, and ground vehicles are built around a network centric architecture that facilitates communication between the onboard, connected, network attached storage (NAS), and other onboard systems. This Ethernet-based communication enables the NAS to do more than just collect data; for example, the networked architecture enables the device to serve files, such as mission maps, mission plans, or boot files, to any network client. By supporting a number of industry standard protocols such as file serving (NFS, CIFS, FTP, HTTP), block (iSCSI), recording (PCAP), and boot (PXE, DHCP), a modern NAS can provide a range of functionality beyond simple storage, but this added functionality increases the risk of data loss or corruption. To meet the challenging needs of todays platforms, NAS systems must provide robust, reliable data storage with minimal loss or corruption in addition to secure encryption, preventing access in the event of system loss or capture.

Basic Modern On-board Network

Most platforms today have an Ethernet-based network that connects network clients to network storage through a switch, as seen in figure 2. Similar to commercial networks, aerospace and defense platforms make use of a range of computing technologies. Network clients can be Intel© or PowerPC® computers and can employ different types of operating systems such as VxWorks®, Linux, or Windows. Due to the varied roles performed by aerospace and defense platforms, network clients must support a wide variety of functions such as mission computing, display, digital signal processing, or sensor management while modern NAS devices are required to support these clients with as much functionality as possible. A modern IP network switch or router that allows any network client to connect to each other, and to the storage device, typically lies at the heart of the onboard network.

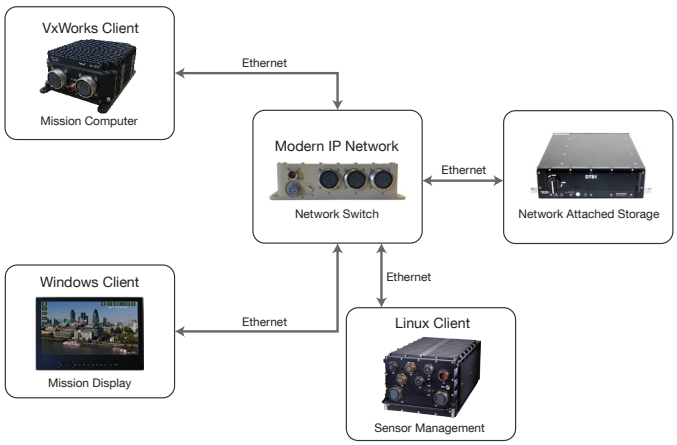

Figure 2: Basic system on board UAV

Added NAS Functionality through Protocol Support

By supporting a range of protocols, NAS devices are flexible, versatile, and interoperable with other networked systems which inherently decreases program costs, risk, and time. Through the support of file serving protocols such as Network File System (NFS), Common Internet File System (CIFS), File Transfer Protocol (FTP), and HyperText Transfer Protocol (HTTP), the device becomes agnostic to computer type and operating system. Because the protocols are industry standard and widely supported, risk of system design error and system incompatibly is greatly reduced. Additionally, any network client can easily store files on, or retrieve files from the NAS during a mission.

Through the support of a block protocol such as Internet Small Computer Systems Interface (iSCSI), legacy systems can be re-deployed. For example, older generations of aircraft may have Fibre Channel (FC) based networks and sensors. When upgrading to an Ethernet network, it may be cost effective to continue using the qualified sensors with FC interfaces. Through the use of iSCSI, it is possible. To learn more, read the white paper: Bridging Legacy Fibre Channel and Modern Ethernet Clients with iSCSI and NAS. In addition to lowering system upgrade costs by enabling the continued use of legacy FC sensors, the iSCSI block protocol enables any Small Computer System Interface (SCSI) initiator to control how the data is arranged in blocks on the SCSI target. In this iSCSI use case, the NAS acts as a SCSI target (like local SCSI and FC disks used to do).

A recording protocol such as packet capture (PCAP) allows Ethernet traffic to be captured for troubleshooting and analysis through common tools like Wireshark®. PCAP is useful for instances where an infrequent error occurs that is very difficult to track down. Often these types of errors show up at random times which can cause real problems for a deployed system. Such errors have been reported in fighter aircraft after years of service.

Finally, support for boot protocols (Preboot Execution Environment (PXE) and Dynamic Host Configuration Protocol (DHCP)) eliminates the need for local storage in each network client. This use of a network boot approach reduces system weight and footprint which is important in any vehicle, but is particularly important for unmanned systems where it can enable additional functionality to be added to the platform. In addition to size and weight reduction, lower client storage also reduces power dissipation, resulting in longer missions. Network booting also eases maintenance by reducing the update time for operating systems and client applications, which in turn increases the up-time for the deployed system. To learn more read the white paper: Using NetBoot to Reduce Maintenance and SWaP-C in Embedded Systems.

While it is clear that multiple protocol support enables additional system functionality and flexibility, these protocols could potentially interfere with each other, resulting in corrupt data if not properly managed.

Isolate NAS Functions with Separate Physical Disks

Industry standard NAS protocols enable clients to connect or mount the remote storage as its own disk. Though the NAS responds to client commands for storing files (such as mission or sensor data), or retrieving (mission plans or maps), the files themselves are arranged by the NAS storage device's file system. Windows-based NAS systems typically use the New Technology File System (NTFS) while Linux-based NAS systems use an EXT4 file system. Though the client dictates which file to save or send, the NAS file system dictates where and how the file is saved on the NAS (figure 3A).

Many IP network clients and storage devices use the iSCSI standard to exchange data. ISCSI is an IP based storage networking standard that carries SCSI commands over a TC/IP network, enabling block level access to remote storage devices (Wikipedia, n.d.). Through iSCSI, the space on a storage server will be regarded as a local disk by a client's operating system (Synology, n.d.).

The NAS acts as a SCSI 'target' and passively awaits instructions from the SCSI 'initiator' (e.g. FC sensor system) (figure 3B). The 'initiator' is active and directs how and where the blocks are stored, bypassing the NAS file system (e.g. EXT4) and increasing the probability of local files being over-written by the block initiator, resulting in data loss. To eliminate this risk, separate NAS disks can be used, removing the possibility of conflict between NAS files and iSCSI block data (figure 3B).

When it comes to Ethernet packet capture, a point file is created, enabling PCAP to co-exist with NAS file services on the same (figure 3D), or virtual disk, but file size could become very large if left unmanaged. If the PCAP file becomes too large, it could encroach on other file types, again resulting in data loss or corruption.

Similarly, boot files can also co-exist with NAS and/or PCAP files on the same or virtual disk. However there are other factors that may suggest a separate physical or virtual disk (figure 3C) is needed. For example, DHCP responses (host IP address, operating system, and application programs) need to be set up by the system designer for each client. It may be desirable from a security viewpoint for the boot files to be located separately from the PCAP or NAS files, and certainly not to co-exist with the block data controlled by the iSCSI initiators.

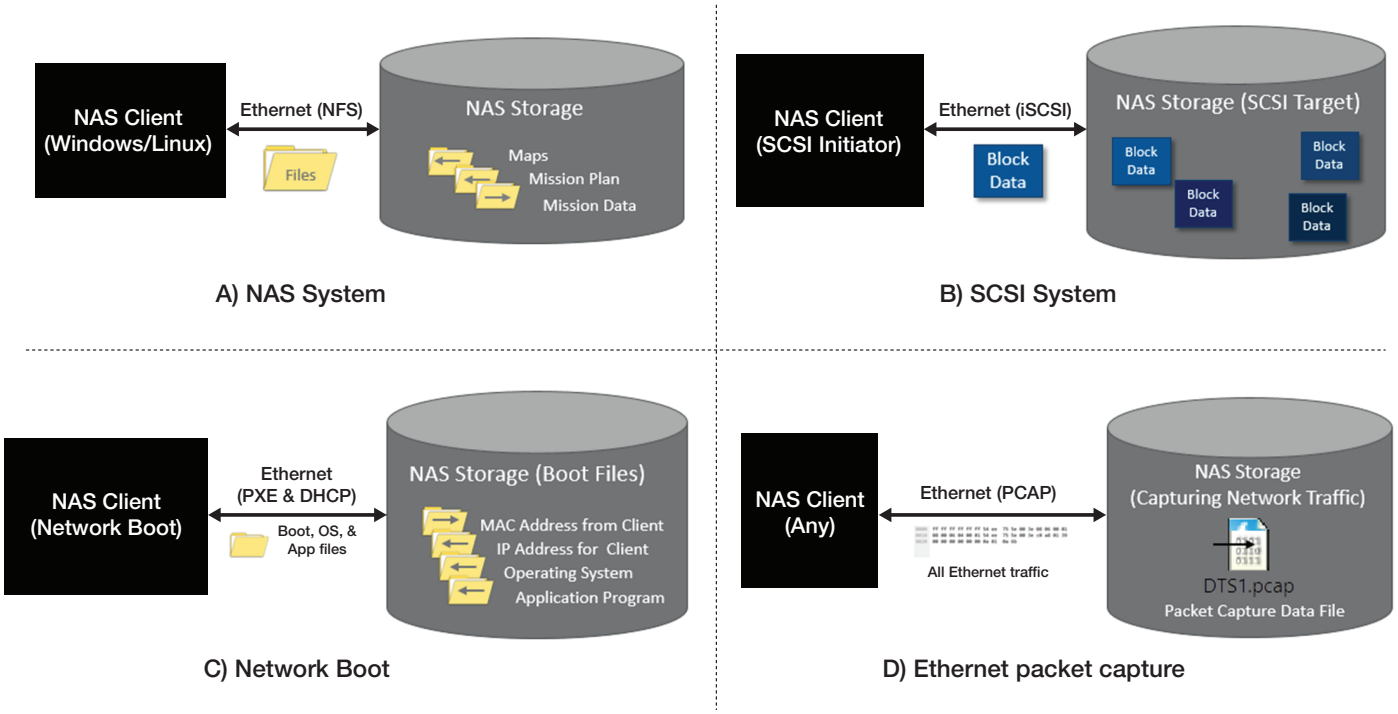

Figure 3: Saving and retrieving using different protocols

With separate physical disks, the NAS files and iSCSI blocks are separated from the boot or PCAP files, reducing the risk of corruption. Separate disks for these functions is a simple solution that avoids interference and potential data loss. A NAS device like the Curtiss-Wright Compact Network Storage, 4-slot (CNS4) (figure 4) has four physical, separate disks. In such a system, each of the four disks can be assigned a different function (NAS, iSCSI, PCAP, and network boot). A NAS device like the Curtiss-Wright Data Transport System 3-slot (DTS3) (figure 4) has three physical disks which can be used for three separate functions.

Figure 4: CNS4 with four separate, physical storage disks and DTS3 with three disks

What if You Only Have One Physical Disk?

With unmanned platforms decreasing in size, NAS devices must be compact. In an effort to reduce size, weight, and power (SWaP), modern NAS devices incorporate only one physical disk (similar to the small Data Transport System 1-slot (DTS1)). The result of NAS, boot, PCAP, and iSCSI protocol support, e.g. figure 5, is a disorganized, insecure approach that will likely lead to data loss or corruption. The stored files can be overwritten and corrupted since the iSCSI initiator can control where it wants blocks to be placed regardless of the local NAS file system. Similarly, the local file system does not know where the remote iSCSI initiator is placing block data, so the block data can be overwritten and corrupted by other files (whether NAS, PCAP, or boot files).

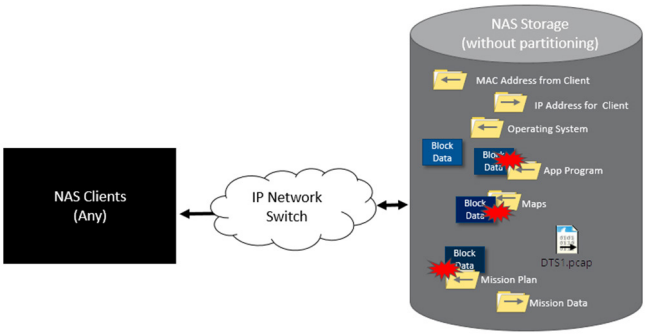

Figure 5: One disk without partitioning

Added Security Through Passphrases for Each Partition

A single physical disk can be divided into virtual disks, one for each function, by using disk partitioning. The iSCSI initiator is free to place block data in its assigned partition without regard to files. With iSCSI assigned its own unique partition or virtual disk, organization is enhanced and risk of cross contamination is eliminated.

Even with separate partitions, what prevents the iSCSI initiator from mounting the NAS partition as a drive? Without additional controls in place, any client can use any partition, creating similar data risks as without a partition. For example, if an iSCSI client could put block data into the NAS partition, it could overwrite the NAS files, or vice versa (figure 6).

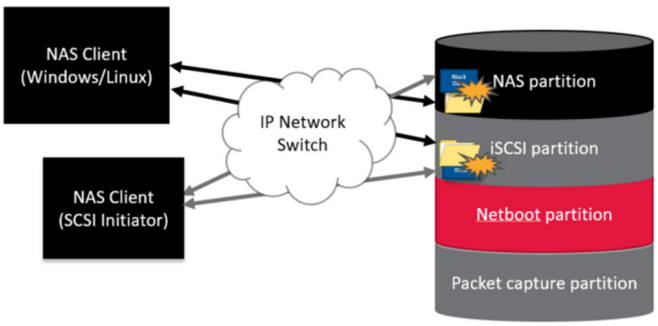

Figure 6: Partitioning without controls

Once separate partitions have been created, a system designer can take advantage of software full disk encryption technologies (SWFDE) to encrypt each partition and assign a unique passphrase for each.

Using Linux Unified Key Setup (LUKS), the most widely used block device encryption solution implemented in Linux based operating systems, unique passphrases can be created for each partition, stopping the flow of traffic from other system functions, as seen in figure 7.

Beyond the benefit of passphrase controls, LUKS provides SWFDE for each partition. LUKS is one of the most secure data encryption and decryption methods on the market. It uses the dm-crypt function and the Advanced Encryption Standard with a 256-bit key (AES-256) that is Federal Information Processing Standard (FIPS) certified for use by U.S. federal departments and agencies to protect up to Top Secret information.

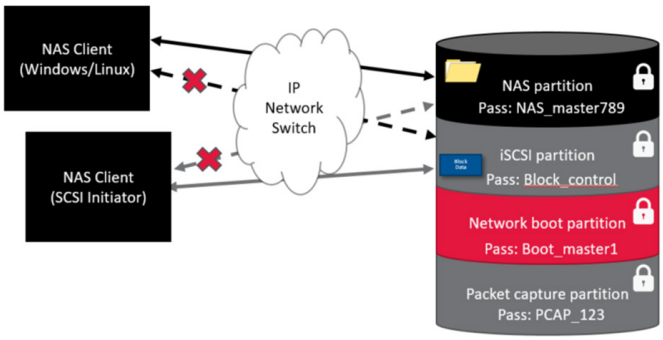

Figure 7: SWFDE partitioning with LUKS

With LUKS and a unique passphrase, the NAS client can only access the assigned NAS partition, where it can retrieve and place files, but cannot access the iSCSI partition and thus cannot corrupt the block data. Similarly, the iSCSI client can only store and retrieve block data from the iSCSI partition and cannot access the NAS partition. Of course, this is the same for both the network boot partition and the packet capture partition as well.

In the example in figure 7, the NAS client has been assigned a partition and given the passphrase 'NAS_master789'. The iSCSI initiator has been assigned a different partition and given the passphrase 'Block_control'. If discipline is maintained, the NAS client does not know the passphrase for any partition other than the assigned one.

Added Security Through Two-Layer Encryption

For rugged defense applications, encrypting sensitive data-at-rest is of utmost importance to eliminate the risk that others could access plain text data in a captured system. Remember the Chinese capture of an unmanned underwater vehicle a few years ago? The number of similar occurrences is expected to rise with the proliferation of unmanned underwater vehicles (UUV), and similar unmanned systems, in 'swarms'.

This heightened concern, in conjunction with the proliferation of data on-board the modern warfare platform, has driven the need for a new breed of encrypted network attached storage devices for data-at-rest applications that not only provide SWFDE but have the added security layer of hardware FDE (HWFDE), in a single device. Curtiss-Wright's DTS1 is the first NAS device on the market that provides two-layer encryption, certified by the National Information Assurance Partnership (NIAP) for Common Criteria (CC), in a rugged, MIL-SPEC chassis (figure 8).

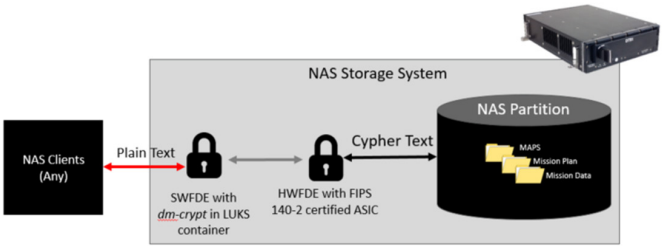

Figure 8: DTS1 provides two-layer, NIAP Common Criteria certified encryption

Having received CC certification, the hardware and software FDE layers used in the DTS1 are currently listed on the United States NIAP Product Compliant List and are now approved to be on NSA's CSfC Components List. Selecting a pre-approved device from the CSfC Components List enables system architects to greatly reduce the time and cost needed to design a COTS encryption solution, which greatly reduces their program risk.

The rugged, small form factor DTS1 can store and protect large amounts of data on helicopters, unmanned aerial vehicles (UAV), UUVs, unmanned ground vehicles (UGV), and ISR aircraft that require the protection of sensitive data-at-rest. The DTS1 is a rugged turnkey network file server that is easily integrated into network-centric systems. Housing one removable memory cartridge (RMC) with two layers of AES-256 bit encryption, the DTS1 provides full and seamless data transfer between one or more networks in separate locations (e.g. from ground to vehicle to ground), ensuring quick data offloading.

In order to minimize SWaP, the DTS1 system has only one physical disk. If the partition scheme suggested above were not implemented, critical data could be corrupted by files writing over block data. With partitioning, the highly useful protocols and the functions they provide can be safely managed while the data is kept separate. By applying LUKS containers to each partition, the client access can be limited to only the assigned partition, assuming passphrases are not shared. The LUKS containers come with the added benefit of SWFDE using AES-256 bit encryption of the data-at-rest. Combine this with the DTS1 capability to encrypt the data with a second distinct HWFDE layer, and you have an incredibly powerful NAS system and peace of mind that the critical data is protected to published standards with certifications to prove it.

Conclusion

With the right protocol support, modern NAS devices can perform a range of useful functions for network clients such as file serving, network booting, iSCSI target emulation, and Ethernet packet capture. The possibility of data loss and corruption increases when multiple functions occur in the same NAS device. This problem is especially true in small, SWaP-optimized NAS devices that store data on one physical disk where the block data stored by iSCSI initiators can overwrite files stored by the local file system.

Separate virtual drives can be created by partitioning a single physical disk, and different partitions can be used for files and block data. This solves the problem of potential data loss or corruption on a single drive by separating the functions into different partitions.

In addition, a system architect may decide that the person assigned to maintain the boot files is not allowed access to the mission files or packet capture files, for example. To ensure clients only have access to their designated partitions, a LUKS container can be created on each partition where each container is assigned a unique passphrase during setup. These unique passphrases are not shared between the responsible persons.

An additional benefit of the LUKS containers (and the unique passphrases) is that the data in each partition is also encrypted prior to storing on the disk. The function dm-crypt encrypts the data-at-rest using the AES-256 bit algorithm.

NAS systems like the DTS1 can provide added security with NSA CSfC approved and Common Criteria certified two-layer encryption, greatly reducing the cost and risk associated with developing an encrypted NSA approved NAS solution. This compact, flexible system reduces the SWaP associated with traditional approaches for data-at-rest protection and is easily integrated into any deployed platform. Curtiss-Wright's DTS1 is the first in a new breed of COTS data protection products made possible by NSA's CSfC initiative. And by employing, partitioning, and encrypted LUKS containers, the data stored by separate functions can be kept separate and protected from unauthorized access. This approach provides system designers with a very powerful tool when designing a deployed Ethernet-based network.

Authors

Paul Davis
Director, Product Management
Data Solutions
Curtiss-Wright Defense Solutions

Elisabeth O'Brien
Manager of Portfolio Marketing
Curtiss-Wright Defense Solutions

Related Content

Products

DTS1 Data Transport System – NIAP Common Criteria certified, NSA CSfC approved

DTS1 Hardware Encryption Common Criteria Certificate

DTS1 Software Encryption Common Criteria Certificate

White Papers

COTS Encryption for Data-at-Rest

Using NetBoot to Reduce Maintenance and SWaP-C in Embedded Systems

Articles

Getting Up to Speed on NSA-approved Two-layer Commercial Encryption

Blogs

Leveraging Commercial Encryption to Reduce Risk and Cost

Case Studies

A COTS Approach to Data-at-Rest Encryption Onboard an Unmanned Underwater Vehicle (UUV)